UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/867,442	05/31/2001	Victor I. Sheymov	741946-27	6583

22204 7590 05/16/2005

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
LEZAK, ARRIENNE M	
ART UNIT	**PAPER NUMBER**
2143	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/867,442	SHEYMOV ET AL.	
	Examiner	Art Unit	
	Arrienne M. Lezak	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Examiner notes that Claims 1-15 have been amended, no Claims have been cancelled and Claims 16-29 have been added. Claims not explicitly addressed herein are found to be addressed within prior Office Action dated 24 September 2004 as reiterated herein below.

Claim Rejections - 35 USC § 112

1. New Claim 28 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, Examiner finds that the claim is unclear as to whether it is dependant or independent in that it is reliant on the steps recited in a different independent claim. Moreover, the independent claim upon which Claim 28 relies is a method claim and Claim 28 is drawn to a computer program product. Proper correction is required. For purposes of examination, Claim 28 will be considered to be a computer program product with claim limitations as recited in independent Claims 1 & 8.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made

to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Newly Amended Claims 1-15 and New Claims 16-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,694,335 to Hollenberg in view of US Patent US 6,735,702 B1 to Yavatkar in further view of US Patent 5,796,952 to Davis.

4. Regarding Newly Amended Claims 1 & 8 and New Claim 28, Hollenberg discloses a distributed network monitoring system, method and computer program product for monitoring a communications network and for detecting an unauthorized communications access attempt into the monitored communications network, (Col. 4, lines 13-59; Col. 5, lines 54-67; Col. 6; Col. 7, lines 1-9; and Col. 8, lines 26-33) comprising:

- one or more distributed hierarchical monitoring systems, (Col. 5, lines 59-67; Col. 11, lines 19-67 & Col 12, lines 1-5); and
- one or more alarm signals, (Col. 5, lines 59-62 & Col. 10, lines 22-37), that represent an unauthorized communications access attempt into one or more portions of the monitored communications network, wherein the one or more distributed hierarchical monitoring systems analyze the unauthorized communications access attempt in response to the unauthorized communications access attempt, and determine a responsive action to the unauthorized communications access attempt, (Col. 6, lines 5-12; Col. 11, lines 19-67 & Col 12, lines 1-5).

5. Though Hollenberg discloses a digital electronic network which communicates or transfers digital information between separate digital computers, systems or nodes, (Col. 4, lines 13-59), which nodes may be any type of computer, (Col. 4, lines 51-59), and which computer nodes are capable of monitoring network integrity and detecting unauthorized attempts to access the same, (Col. 8, lines 26-33), Hollenberg does not specifically teach the sending of a mechanism for determining a source of the unauthorized communications access attempt in response to the unauthorized communications access attempt.

6. Yavatkar discloses a system for diagnosing network intrusions, which uses agents to identify the source of attacks, (unauthorized access attempts), (Yavatkar - Col. 3, lines 25-67 & Col. 4, lines 1-48). Davis further enumerates a specific tracking program for determining the source of the unauthorized communications access attempt, which program is capable of being embedded into files, (Davis - Col. 4, lines 1-67 & Col. 5, lines 1-56). It would have been obvious to one of ordinary skill in the art at the time of invention by Applicant to incorporate the Yavatkar and Davis systems for diagnosing network intrusions into the Hollenberg system for intrusion detection as the Hollenberg system teaches computer nodes capable of sensing any attempt to gain unauthorized access, (Hollenberg – Col. 6, lines 8-12). Further, the Yavatkar enumerates a need for a system and method for quickly and accurately collecting information about an attack on a distributed network, (Yavatkar – Col. 2, lines 44-50), and the Davis specifically teaches a tracking program, which tracking program could obviously be used for accurately collecting any type of information on a distributed

network. Thus, Newly Amended Claims 1 & 8 and New Claim 28 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

7. Regarding New Claims 17-21 & 23-27, the combined teachings of Hollenberg, Yavatkar and Davis are relied upon as noted herein. As noted above, Yavatkar clearly teaches a determining mechanism inclusive of an obviously concealed agent, (per pending Claims 17 & 23), wherein the agent reveals the path of the unauthorized access attempt, (per pending Claims 19 & 25), (Yavatkar - Col. 3, lines 25-67 & Col. 4, lines 1-48). Additionally, Davis clearly teaches a program embedded (concealed) in a file (web page) sent to a client, (per pending Claims 20, 21, 26 & 27), (Davis - Col. 4, lines 1-67 & Col. 5, lines 1-56), which file could also obviously be identified/embedded with a flag, (per pending Claims 18 & 24), particularly in light of the Yavatkar agents for identification of the same. Moreover, Examiner notes that any program or agent used for path detection would obviously need to be concealed to avoid detection by the individual attempting the unauthorized access. Thus, New Claims 17-21 & 23-27 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

8. Regarding Amended Claims 2 & 9 and New Claim 29, the combined teachings of Hollenberg, Yavatkar and Davis are relied upon as noted herein. Hollenberg further discloses a distributed network monitoring system and method further comprising a monitoring device that monitors information on one or more monitored communication networks, (or portion thereof – per pending Claim 9), (Col.11, lines 19-67 & Col. 12,

lines 1-5). Thus, Amended Claims 2 & 9 and New Claim 29 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

9. Regarding Amended Claims 3, 10 & 11, the combined teachings of Hollenberg, Yavatkar and Davis are relied upon as noted herein. Hollenberg further discloses a distributed network monitoring system and method further comprising an intrusion analysis system that receives the one or more alarm signals and at least one of determines the origin of the unauthorized communications access attempt, logs communications and evaluates the threat of the unauthorized communications access attempt, (Col. 6, lines 5-12; Col. 11, lines 19-67; and Col. 12, lines 1-5). Though Hollenberg does not specifically enumerate the restriction of logging, (data collection), based on an analysis of the unauthorized access attempt, (per pending Claim 11), Examiner notes that the same would have been obvious to one of ordinary skill in the art at the time of invention by Applicant, as the prior art teaches monitoring and responding to unauthorized access attempts and collecting data about the same. It would be obvious within such a monitor/response system to have different levels of response based on the level of threat. Further, in some instances, recording of access attempt data may not be necessary, (i.e. false alarm). Additionally, Examiner notes that both Yavatkar and Davis teach tracking systems, which systems gather and report report data. Thus, Amended Claims 3, 10 & 11 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

10. Regarding Amended Claims 4 & 12, the combined teachings of Hollenberg, Yavatkar and Davis are relied upon as noted herein. Hollenberg further discloses an

intrusion interaction system capable of communicating with the origin of the unauthorized communications access attempt, (Col. 30, lines 27-67 & Col. 31, lines 1-59). Examiner notes that a GPS system allows for direct communication with a monitoring station, as well as a "listen in" functionality, which communication functionality allows the monitoring station to communicate with any unauthorized vehicle occupant. Thus, Amended Claims 4 & 12 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

11. Regarding Amended Claims 5 & 13 and New Claims 16 & 22, the combined teachings of Hollenberg, Yavatkar and Davis are relied upon as noted herein. Hollenberg further discloses an escalation determination system that, based on an evaluation the unauthorized communications access attempt and a comparison to one or more other unauthorized communications access attempts, forwards information regarding the unauthorized communications access attempt to the one or more of the one or more hierarchical monitoring systems, (Col. 5, lines 54-67; Col. 6; Col. 7, lines 1-8; Col. 11, lines 19-67; and Col. 12, lines 1-5). Examiner notes that the evaluation and comparison of unauthorized attempts would have been obvious within a monitoring system with data storage capability, like Hollenberg, wherein it would have been obvious to compare and evaluate each "breach of security" situation on an individual basis in order to determine the true nature of the threat and thus act accordingly. Thus, Amended Claims 5 & 13 and New Claims 16 & 22 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

12. Regarding Amended Claims 6 & 14, the combined teachings of Hollenberg, Yavatkar and Davis are relied upon as noted herein. Hollenberg further discloses a distributed network monitoring system and method wherein the one or more alarm signals is generated by one or more recipients of the unauthorized communications access attempt, Col. 5, lines 59-67; Col. 11, lines 19-67; and Col. 12, lines 1-5). Thus, Amended Claims 6 & 14 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

13. Regarding Amended Claims 7 & 15, the combined teachings of Hollenberg, Yavatkar and Davis are relied upon as noted herein. Hollenberg further discloses a response system that communicates information regarding the unauthorized communications access attempt to one or more of a monitored site, (Col. 11, lines 19-67 & Col. 12, lines 1-5), and obviously a law enforcement agency. Examiner notes that a GPS system provides transmitted information, which information allows a control center to take appropriate action, such as dispatching law enforcement. Thus, Amended Claims 7 & 15 are found to be unpatentable over the combined teachings of Hollenberg, Yavatkar and Davis.

Response to Arguments

14. Applicant's arguments filed 21 January 2005, have been fully considered but they are not persuasive. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections

made. Further, they do not show how the amendments avoid such references or objections.

15. Regarding Applicant's argument that Hollenberg is concerned with an unauthorized physical access attempt, (as opposed to a "communications" access attempt), Examiner notes that during the interview it was noted that Hollenberg does indeed disclose a communication network wherein computer nodes communicate with one another as part of intrusion detection, (Col. 6, lines 1-52). Examiner maintains that this inter-nodal communication on it's own or in combination with (or as applied to) the Yavatkar and Davis distributed computer networks clearly renders Applicant's claims unpatentable, as noted herein above.

16. Thus, as Examiner has completely addressed Applicant's amendment, and finding Applicant's arguments do not show how the amendments avoid such references or objections, Examiner hereby rejects all amended and newly added claims in their entirety as noted herein above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arrienne M. Lezak whose telephone number is (571)-272-3916. The examiner can normally be reached on M-F 8:30-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571)-272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Arrienne M. Lezak
Examiner
Art Unit 2143

AML

BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER